NEW CENELEC STANDARDS & CSM-RA
AGENDA

- New EN 501xx Standards
- What is new/changed/improved
- The use of CENELEC in CSM-RA process
CENELEC & CSM-RA TIMELINE

- **ENV50126**
  - 1995

- **EN50126**
  - 1999

- **EN50128**
  - 2000

- **EN50129**
  - 2001

- **EN61508**
  - 2003

- **EN50126**
  - 2010

- **EN50128**
  - 2011

- **EN61508**
  - 2017

- **EN50126**
  - 2018

- **ENV50126**
  - 2010

- **EN50126**
  - 2012

- **TR50126-2**
  - 2006

- **TR50126-3**
  - 2007

- **TR50126-2**
  - 2015

- **TSI**
  - 2010

- **CSM-RA 352/2009**
  - 2017

- **CSM-RA 402/2013**
  - 2017

- **CSM-RA 1136/2015**
  - 2017
OVERVIEW OF CURRENT RAILWAY SAFETY STANDARDS

**System Level**

**EN 50126**
The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

**EN 50129**
Communication, signalling and processing systems – Safety related electronic systems for signalling

**EN 50128**
Communications, signalling and processing systems - Software for railway control and protection systems

**Guidance**

**TR 50126-2**
Guide to the application of EN 50126 for safety

**TR 50126-3**
Guide to the application of EN 50126 for rolling stock

**TR 50506-1**
Guide to the application of EN 50129 – Part 1: Cross Acceptance

**TR 50506-2**
Guide to the application of EN 50129 – Part 2: Safety Assurance

**SubSystem (Product)**

**EN 50126**
The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

**EN 50129**
Communication, signalling and processing systems – Safety related electronic systems for signalling

**EN 50128**
Communications, signalling and processing systems - Software for railway control and protection systems

**Guidance**

**TR 50126-2**
Guide to the application of EN 50126 for safety

**TR 50126-3**
Guide to the application of EN 50126 for rolling stock

**TR 50506-1**
Guide to the application of EN 50129 – Part 1: Cross Acceptance

**TR 50506-2**
Guide to the application of EN 50129 – Part 2: Safety Assurance
OVERVIEW OF NEW RAILWAY SAFETY STANDARDS

System Level

EN 50126
The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

EN 50129
Communication, signalling and processing systems – Safety related electronic systems for signalling

EN 50128
Communications, signalling and processing systems - Software for railway control and protection systems

Guidance

EN 50126-2
Systems Approach to Safety

TR 50506-1
Guide to the application of EN 50129 – Part 1: Cross Acceptance

TR 50506-2
Guide to the application of EN 50129 – Part 2: Safety Assurance
SAFETY STANDARDS RELATIONSHIPS

Entire Railway system

General standard (generic)

Railway sub-system / Product

Specific sector / application

EN 50126

EN 50129
System
HW+SW

EN 50128
SW

EN 61508 “FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS”


IEC 62061, Safety of machinery Functional safety of electrical/electronic/programmable control systems

Railway Applications

Railway signalling

Other sectors (e.g. machinery / process control)

Other

Where no other sector/application exists

NEW CENELEC STANDARDS & CSM-RA

Adapted after EN 50129 / IEC WG group
RAILWAY SAFETY STANDARDS - SUBSYSTEM

SC9X / S-509

EN 50126-1 & 2
Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
2017

EN 50129
Communication, signalling and processing systems - Safety related electronic systems for signalling
2018

EN 50128
Communications, signalling and processing systems - Software for railway control and protection systems
2011

EN 50155
Electronic equipment used on rolling stock
2017

EN 50657
Rolling stock applications - Software on board of rolling stock, excluding railway control and protection applications
2017

EN 50562
Process, measures and demonstration of safety for electric traction systems
2018

SC9XA

SC9XB

SC9XC

Signalling
Rolling Stock
Fixed Installation

NEW CENELEC STANDARDS & CSM-RA
2017
EN 50126 OLD & NEW IN COMPARISON

**Similarities**
- System approach for RAMS
- Risk based approach
- RAMS lifecycle
- Safety demonstration principles

**New/changed**
- More mature and consistent
- CSM-RA approach
  - Multilevel system approach (hierarchies)
  - Aligned risk evaluation
- Safety demonstration
- Safety requirements Spec.
- Guidance integrated part
- Clear linkage to TSI

**Improved/detailed**
- Clear hazard identification and classification
- Classification of safety requirements
- Method to derive THR from statistics
- Safety Case structure
  - Modularity
  - Handling of product/Generic / specific Application
- Safety Apportionment methods
- Key system safety roles & responsibilities

Ramboll
PRODUCTS IN CENELEC PROCESS

**EN 50126**
- Provide the overall process for development of products
- Lifecycle
- Hazard identification and management
- Safety requirements identification and apportionment
- Safety target (THR, TFFR, SIL)
- Implementation evidence
- Documentation

**50129/50128**
- Provide the process for development of products
- Tailored system/hardware/software development process
- Detailed analysis of failure and hazard control
- SIL demonstration
- Product specific implementation evidence
- Product specific documentation
EN 50129

General
1: Scope
2: Normative reference
3: Definition

4: Overview

5: Requirements for Developing electronic systems

6: Requirements for external elements

7: Safety Case

Annex C
HW component failure modes

Annex A
Safety Integrity Level (SIL)

Annex B
Management of faults

8: Acceptance and subsequent phases

Annex E
SIL-based techniques

Annex F
Programmable Components

Bibliography
CSM-RA VERSUS EN50126

CSM-RA

• Focus on a change
• Significance
• Emphasis on hazard identification & control
• Hazard normally controlled by well known measures
• Independent safety assessor as NSA proxy

EN 50126

• Can be applied for changes and products
• Always applicable
• Life cycle approach in hazard identification and control
• Generic control of hazards
• Verification and validation process
• Independent safety assessor to ensure process
• Functional Safety & Safety Integrity
• RAM (dependability)
CSM-RA SUPPORTED BY EN50126

CSM-RA
- The Legal framework
- System definition
- Risk Management process
- Require systematic process
- Require documentation for hazard control

EN 50126
- Hierarchical system definition model
- Detailed risk management process & evaluation principles
- The systematic process
  - Standard lifecycle to be tailored to project
  - Detailed risk management process
  - Engineering process requirements
- Provide the principles for safety documentation
  - Safety Case structure
  - Verification & Validation process

The Good Process
EN 50126 LIFECYCLE COMPARED TO CSM-RA PROCESS

1. Concept
2. System definition and Operational Context
3. Risk Analysis and Evaluation
4. Specification of System Requirements
5. Architecture and Apportionment of System Requirements
6. Design and Implementation
7. Manufacture
8. Integration
9. System Validation
10. System Acceptance
11. Operation and Maintenance
12. De-commissioning and Disposal

CSM-RA

Risk Assessment
- System Definition
- Hazard Identification and classification
- Code of Practice
- Similar Reference System
- Explicit Risk Estimation
- Risk Evaluation vs risk acceptance criteria
- Safety Requirements
- Demonstration of Compliance with Safety Requirement

Hazard Management
System Definition
Risk analysis
Risk evaluation
System requirements
Safety Measures & Safety requirements
- Code Of practice
- Reference system
- Functional/technical/context
Hazard analysis
 Demonstration of compliance

Railway Duty Holder’s responsibility
Proposer

Legal framework
Contractual Arrangement

Actor
Supplier's Responsibility

CSM-RA

Additional Hazards
Application Conditions

CENELEC
System
Sub System
Products

NEW CENELEC STANDARDS & CSM-RA
2017
SYSTEM DEFINITION

Contextual Requirements
*The operational environment*

Functional Requirements
*What the system shall do*

Technical Requirements
*Ensure the system function*
EXAMPLE

Trains too close -> separate

Hazard related to Generic Appl.

Block sections
Indicate free/occupied

Hazard related to Generic Appl.

Axle counter
Indicate free while occupied

Hazard related to Specific Appl.

Failures/Hazards in Product

CSM-RA

EN50126

EN50129

EN50128

Generic Application SC

Specific Appliance SC

Generic Product SC

Specific
Proposer’s Hazard Record

Allocation of hazards

Implementation

Supplier Hazard Log

CSM-RA
CENELEC

System Definition

Register

Specific log

CLOSE

Safety Demonstration

CSM-RA
CENELEC

Safety Documentation

Specific Appl. Safety Case(s)

EN50126

EN50126

EN50129

Generic Appl. Safety Case(s)

Generic Product Safety Case(s)

EN50129

EN50128

NEW CENELEC STANDARDS & CSM-RA
2017
APPLICATION OF CENELEC STANDARDS ON SYSTEM/SUBSYSTEM LEVEL

Hazard 1  Hazard 2  Hazard 3

Hazards identified in CSM-RA

EN 50126 systematic process

EN 50129 System Integration

EN 50128 Software development process
SIL requirement

EN 50129 Hardware development process

System

SystemIntegration

Hardware  Software
HAZARD RATES & SIL - PRINCIPLE

Safety functionality

Hazard not controlled by system
Hazard not fully mitigated
System Failure

Safety Integrity (SIL)

Functional Safety System
SAFETY INTEGRITY

SIL Qualitative Measures

Quality Management Conditions

Safety Management Conditions

Technical Safety Measures

Compliance to the Safety Integrity measures

SIL Quantitative Measures

Demonstration of Quantitative Targets

Tolerable Functional Failure Rate

$10^{-9} \leq \text{TFFR} < 10^{-8}$

$10^{-8} \leq \text{TFFR} < 10^{-7}$

$10^{-7} \leq \text{TFFR} < 10^{-6}$

$10^{-6} \leq \text{TFFR} < 10^{-5}$

SIL Qualitative Measures

Defined in sector specific standard EN50129/EN50128

Compliance to Basic Integrity measures

SIL

4

3

2

1
V & V INDEPENDENCE ARRANGEMENTS

SIL 4 / SIL 3
(Vital)

OR

SIL 2 / SIL 1
Basic Integrity
CENELEC & CSM-RA

New EN 50126 & EN 50129

- No Contradiction with CSM-RA – but a good Code of Practice for the process

- CENELEC -> provide the good practice

- Fill-in on products
THANK YOU

QUESTIONS?

STIG MUNCK

SGM@RAMBOLL.DK
+45 5161 6375